

REPLY'S OFFER FOR BUSINESS SECURITY

Reply has an integrated, consistent and complete offer to support its Clients in the development of suitable strategies and in the implementation of adequate solutions for the effective management of Business Security & Data Protection. Our mission is to enable our Clients' companies to establish trust-based relationships with their interlocutors and enable the performance of their business processes, by taking into consideration all aspects relating to risks associated to an IT System.

THE DELIVERY MODEL

Thanks to the contribution of over 200 employees, highly specialized in the main technologies and solutions, in possession of over 200 certifications, and working actively at the most important International bodies and institutions, the Reply offer in the field of Information Security covers the following sectors:

- **Professional Services** for the development of ICT security solutions and countermeasures of the following types:
 - Infrastructural, with Network and System Security solutions
 - Application, with SOA and Web2.0 Security solutions, Code Review, etc ...
 - Digital Identity Management, with Identity and Access Management solutions
- **Consulting Services** in fields like:
 - Security Strategy & Compliance
 - Security Governance
 - Security Awareness and Training
- **Managed Security Services** delivered round-the-clock by our Security Operation Centre
- **IT Fraud Management** through Anti-phishing e Transaction monitoring controls
- **Security Assessment** in order to assess security levels

The delivery model allows the integration and synergy of all these different aspects of IT security, which are strictly interlinked in order to be able to thoroughly cover the different aspects of Business Security.

BUSINESS SECURITY

BUSINESS SECURITY ASPECTS. To develop a Security Program covering all company aspects and focusing mainly on business aspects, it is necessary to have a methodological approach enabling to start from the analysis of the current situation, of regulatory requirements and security objectives, in order to set up a solution implementation strategy. Such need stems from the fact that Information Security covers different fields: technological, functional, organizational, legal and economic.

Spike Reply, a company of the Reply Group, specialized in Security issues, develops Business Security projects using a proprietary methodology able to adapt to the Client's specific requirements and checked using the best-of-breed technology solutions available on the market.

ICT SECURITY PROFESSIONAL SERVICES

PLANNING: This type of activity is essential to plan, assess and select the best solutions among the possible technological or architectural offers available on the market. These offers are compared with the real protection needs of the client, in order to obtain the best RoI for that specific solution. The in-depth knowledge acquired on the ground allow Reply to master particularly complex architectures in a multi-platform environment developed for different Information Security areas: Network Security, System Security, Application Security, Data Security, User Profile Security in highly critical environments, as well as in high-performance environments.

DEVELOPMENT: A company policy has no real value if the technological countermeasures which have been planned are not developed and implemented in a careful and skilful way. Reply's strongpoint lies in the planning and development of ICT solutions, thanks to its excellent technological features, widely recognized by the market. Thanks to the distinctive competences and the strong synergies within the group, Reply is able to develop different Security solutions, thus offering turnkey solutions.

MAIN THEME AREAS: The main theme areas covered in this field are:

- Network & System Security:
 - Perimetral Security and IDS/IPS
 - Hardening
 - High Reliability Systems
 - Log management and Audit (SIEM)
- Application Security:
 - Safe Coding
 - Code Review
 - Digital Signature / PKI

- SOA Security
- Web2.0 Security
- Application and Web Firewall
- Data Security:
 - Content Filtering
 - Data Encryption
 - Desktop Security
 - Database Security
 - Data Masking
 - DLP (Data Loss Prevention)
- User Profile Security: Analysis and Planning of Identity and Access Management Solutions starting from a profile and process models up to the implementation of support technological services like:
 - Identity Management, Role Management, User Provisioning
 - Enterprise and Web Single Sign-on, Strong Authentication
 - Federation

CONSULTING SERVICES

CONSULTANCY: Reply's consulting competence applies to all our projects, since the best security architecture risks to be inefficient if it is not followed and managed by people sharing the same principles, the same procedures and behaving in a consistent way, thus complementing the technologies and the physical measures adopted, in an effort to protect the company's critical information against internal and external threats. Reply works in strict contact with the client's company and its environment, in order to define principles, general policies and security objectives, as well as the security functional organization, by detecting which are the people involved and detailing the relevant roles, as well as specific responsibilities and procedures.

MAIN THEME AREAS: The main theme areas covered in this field are:

- Security Strategy & Compliance:
 - Risk Analysis / Business Impact Analysis
 - Security Integrated Plan (Security Blueprint, Security Roadmap)
 - Business Continuity & Disaster Recovery Plans and Systems (BS25999)
 - Information Security Management Systems (ISMS; ISO27001)
 - Documentation System (General Policies and Security Operational Procedures)
 - Privacy Compliance (D.Lgs 196/03): development of DPS and regulatory system
 - Compliance with laws, regulations and best practices (SOX, L.231, ABI, Basilea II, PCI-DS, ITIL ...)
 - Development and implementation of Internal Competence Centre and/or

Security Operation Centre

- Security Governance:
 - Secure Application Building (SSDLC; support to the SW development team; Code Review)
 - Monitoring dashboard and Security Indicators (Security KPI/KRI/KPO)
 - Vulnerability & Patch Management
 - IT Accident Management
 - Security Awareness and Training with tailor-made courses, on the basis of the client's specific needs

MANAGED SECURITY SERVICES

SECURITY OPERATION CENTER (SOC). The Communication Valley Security Operation Center (SOC), a Spike Reply's associated company, is a physical and logical unit, the only one in Italy, specialized in the delivery of managed and professional IT security services. SOC works for a number of organizations and, as a competence center, is in possession of over one hundred certifications. It is a true "control tower", manned 24 hrs a day, 365 days a year by a security team made up by analysts, systemists and testers, specialized in real time monitoring, security system management and security assessment respectively. SOC avails itself of an exclusive infrastructure (Enterprise Security Management), made up by a series of applications for: security event management, attack patterns recognition, technology upkeep, Knowledge and Asset Management. SOC interacts and share service outputs with the client, through a web-based portal, easy to use and rich in contents.

SOC delivers the main IT Security Services which make up our Managed Security Services offer:

- **Security Information and Event Management**, for the planning and development of solutions for the collection and correlation of reliable data on the use of network and its components, as well as of all information necessary to optimize resources, correct configurations and inhibit behaviours that may compromise the efficiency of the Information System
- **Security Monitoring**, for the control and detection of network anomalies.
- **Network and Security Device Management**, for the operational management of network and security systems.
- **Early Warning**, for the prompt management of escalations in case of meaningful events.
- **Policy Compliance**, to adapt IT systems to the risk factor chosen to comply with company rules, standards and regulations.
- **Security Policy**, to periodically check and minimize the IT systems exposure, with regards to their vulnerability level.

IT FRAUD MANAGEMENT

FRAUD MANAGEMENT. Fraud is an intentional damage caused for one's own interests, in order to obtain non-authorized benefits (money, property etc.) in fields such as legal, commercial, fiscal, currency-related, sports, food and banking.

"Online Fraud" means any type of fraud committed through the use of IT tools.

The majority of fraud cases concern identity theft and impersonification in the credit, commercial, insurance and telecommunications sectors.

Our reply to online frauds revolves around two main activities:

- Anti-phishing, to minimize the risk of identity theft;
- Transaction monitoring, to block any illegal activity carried out with illegally acquired identity data.

ANTI-PHISHING. Phishing is an online fraud technique using various methods to cheat the user and induce him/her to disclose personal and sensitive information (username, password, credit card number etc.).

Anti-phishing activities are performed using a series of specialized proprietary tools and offering support, 24/7, by specialists working in our SOC (Security Operations Center). Our solution includes the following benefits: preliminary analysis of domain registration, round-the-clock phishing incident detection, analysis of each incident, targeted takedown of the phishing network, credential dilution and insertion of bait credentials.

TRANSACTION MONITORING. Transaction monitoring is a powerful tool in order to:

- Monitor online activities in a transparent way (both during the login and post-login phase);
- Detect high-risk activities, report and recommend appropriate actions;
- Empower financial institutions to effectively investigate the reported high-risk activities;

The indicators used by the system, which establish the calculation of the risk level during a transaction concern:

- User Profile;
- IP Profile;
- Mechanism Profile.

By gathering a high number of indicators for each profile type, the system establishes a risk level to which a specific action may then be associated.

SECURITY ASSESSMENT

THE ASSESSMENT: Once the best solution has been chosen and developed, it is important to continuously monitor the system through Assessment sessions. The discovery of new intrusion techniques and new ways to counteract and minimize attacks require the periodical assessment of the IT system security; this is necessary in order to maintain correct parameters of confidentiality, integrity, availability, authenticity, non-rejection and privacy. This assessment is carried out in different ways, according to the specific objective one wishes to attain: systems and/or applications (EthicalHacking) external assessment; configuration internal assessment; information system passive test, through configuration file assessment and interviews with administrators and programmers; verification tests of operational and organizational procedures, of manuals and of their actual implementation. These activities naturally lead to the comprehensive management of the security level maintenance achieved through the delivery of Managed Security Services by our Security Operation Center (SOC).

MAIN THEME AREAS: The main theme areas covered in this field are:

- ICT Security Assessment – Security Check-Up (general assessment of security aspects (LOFTA))
- Vulnerability Assessment (identification of IT security vulnerabilities)
- Ethical Hacking / Penetration Test (identification and practical assessment of information gaps)



Within the Reply Spa Group, Spike Reply and Communication Valley are companies specialized in the field of Security and Personal Data Protection. Reply developed a comprehensive, integrated and consistent offer, in order to tackle any aspect of risks associated to an information system: from detection of threats and vulnerabilities, to the definition, planning and implementation of technological, legal, organizational, insurance or risk retention counter-measures. Communication Valley is a Managed Service Provider specialized in the security management of complex networks. Its solutions are applied to all types of data and voice networks: wireless and wired, traditional and VoIP. Its portfolio includes security assessment, security device management and real time monitoring activities. Communication Valley can boast a Security Operations Center where security specialists are active H24x365.

The Reply mission is to allow its customers to perform their business in a secure environment, thus supporting them during the development and implementation of adequate strategies and solutions, for an effective management of Information Security.

Spike Reply
www.reply.eu